

501P0370US00 #4

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

J1044 U.S. PTO  
09/801802  
03/09/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

2000年 3月14日

出 願 番 号  
Application Number:

特願2000-069697

出 願 人  
Applicant (s):

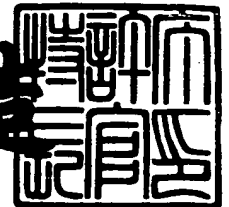
ソニー株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年12月22日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2000-3106137

【書類名】 特許願

【整理番号】 9900878406

【提出日】 平成12年 3月14日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/16

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
    内

    【氏名】 郷 直美

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
    内

    【氏名】 栗原 章

【特許出願人】

    【識別番号】 000002185

    【氏名又は名称】 ソニー株式会社

    【代表者】 出井 伸之

【代理人】

    【識別番号】 100082131

    【弁理士】

    【氏名又は名称】 稲本 義雄

    【電話番号】 03-3369-6479

【手数料の表示】

    【予納台帳番号】 032089

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体

【特許請求の範囲】

【請求項 1】 第 1 の情報処理装置を認証する第 1 の認証手段と、  
第 2 の情報処理装置を認証する第 2 の認証手段と、  
前記第 1 の情報処理装置からの、前記第 2 の情報処理装置を特定するデータおよび鍵の送信要求の受信を制御する受信制御手段と、  
前記第 2 の情報処理装置を特定する前記データに基づき、前記第 2 の情報処理装置に前記鍵の送信要求を送信するとともに、前記第 2 の情報処理装置から前記鍵を受信するように通信を制御する通信制御手段と、  
前記第 1 の情報処理装置への前記鍵の送信を制御する送信制御手段と  
を含むことを特徴とする情報提供装置。

【請求項 2】 第 1 の情報処理装置を認証する第 1 の認証ステップと、  
第 2 の情報処理装置を認証する第 2 の認証ステップと、  
前記第 1 の情報処理装置からの、前記第 2 の情報処理装置を特定するデータおよび鍵の送信要求の受信を制御する受信制御ステップと、  
前記第 2 の情報処理装置を特定する前記データに基づき、前記第 2 の情報処理装置に前記鍵の送信要求を送信するとともに、前記第 2 の情報処理装置から前記鍵を受信するように通信を制御する通信制御ステップと、  
前記第 1 の情報処理装置への前記鍵の送信を制御する送信制御ステップと  
を含むことを特徴とする情報提供方法。

【請求項 3】 第 1 の情報処理装置を認証する第 1 の認証ステップと、  
第 2 の情報処理装置を認証する第 2 の認証ステップと、  
前記第 1 の情報処理装置からの、前記第 2 の情報処理装置を特定するデータおよび鍵の送信要求の受信を制御する受信制御ステップと、  
前記第 2 の情報処理装置を特定する前記データに基づき、前記第 2 の情報処理装置に前記鍵の送信要求を送信するとともに、前記第 2 の情報処理装置から前記鍵を受信するように通信を制御する通信制御ステップと、

前記第 1 の情報処理装置への前記鍵の送信を制御する送信制御ステップと  
を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納され  
ているプログラム格納媒体。

【請求項 4】 第 1 の情報提供装置を認証する認証手段と、  
前記第 1 の情報提供装置への、鍵を提供する第 2 の情報提供装置を特定するデ  
ータおよび前記鍵の送信要求の送信を制御する送信制御手段と、  
前記第 2 の情報提供装置から前記第 1 の情報提供装置が提供を受け、送信した  
前記鍵の受信を制御する受信制御手段と  
を含むことを特徴とする情報処理装置。

【請求項 5】 第 1 の情報提供装置を認証する認証ステップと、  
前記第 1 の情報提供装置への、鍵を提供する第 2 の情報提供装置を特定するデ  
ータおよび前記鍵の送信要求の送信を制御する送信制御ステップと、  
前記第 2 の情報提供装置から前記第 1 の情報提供装置が提供を受け、送信した  
前記鍵の受信を制御する受信制御ステップと  
を含むことを特徴とする情報処理方法。

【請求項 6】 第 1 の情報提供装置を認証する認証ステップと、  
前記第 1 の情報提供装置への、鍵を提供する第 2 の情報提供装置を特定するデ  
ータおよび前記鍵の送信要求の送信を制御する送信制御ステップと、  
前記第 2 の情報提供装置から前記第 1 の情報提供装置が提供を受け、送信した  
前記鍵の受信を制御する受信制御ステップと  
を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納され  
ているプログラム格納媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報提供装置および方法、情報処理装置および方法、並びにプロ  
グラム格納媒体に関し、特に、コンテンツを復号する鍵を提供するか、または暗号  
化されているコンテンツを利用する情報提供装置および方法、情報処理装置およ  
び方法、並びにプログラム格納媒体に関する。

## 【0002】

## 【従来の技術】

図1は、従来のデジタルデータ伝送システムの構成を示す図である。パーソナルコンピュータ1は、ローカルエリアネットワークまたはインターネットなどから構成される通信ネットワーク4に接続されている。パーソナルコンピュータ1は、コンテンツサーバ22から受信した、またはCD (Compact Disc) から読み取った楽音のデータ（以下、コンテンツと称する）を、所定の圧縮の方式（例えば、ATRAC3（商標））に変換するとともにDES (Data Encryption Standard) などの暗号化方式で暗号化して記録する。

## 【0003】

パーソナルコンピュータ1は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

## 【0004】

利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に利用することができるポータブルデバイス (Portable Device (PDとも称する)) の台数（後述する、いわゆるチェックアウトできるPDの台数）を示す。利用条件のデータに示される数だけコンテンツをチェックアウトしたときでも、パーソナルコンピュータ1は、そのコンテンツを再生できる。

## 【0005】

パーソナルコンピュータ1の表示操作指示プログラム11は、パーソナルコンピュータ1が記録しているコンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、チェックアウトの指示などを入力して、SDMI (Secure Digital Music Initiative) の規格に準拠したソフトウェアモジュールであるLCM (Licensed Compliant Module) 12にその指示に対応したチェックアウトなどの処理を実行させる。

## 【0006】

パーソナルコンピュータ1のLCM12は、コンテンツの不正な2次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から

構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【0007】

LCM12は、パーソナルコンピュータ1に接続された機器が正当であるかの認証を行い、安全な方法でコンテンツの移動の処理などを実行する。コンテンツの移動の処理などに伴い、LCM12は、必要な鍵を生成して、鍵を管理し、コンテンツを暗号化し、または接続されている機器との通信を制御する。

【0008】

また、LCM12は、装着されているポータブルメディア3の正当性をチェックして、サーバ5が指定した利用条件をコンテンツ（暗号化されている）に付加して、コンテンツを記録させる。

【0009】

パーソナルコンピュータ1のLCM12は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ（例えば、曲名、または利用条件など）と共に、接続されているポータブルデバイス2に供給するとともに、ポータブルデバイス2に供給したことに対応して、供給したコンテンツに対応する利用条件のデータを更新する（以下、チェックアウトと称する）。より詳細には、チェックアウトしたとき、パーソナルコンピュータ1が記録している、そのコンテンツに対応する利用条件のデータのチェックアウトできる回数は、1減らされる。チェックアウトできる回数が0のとき、対応するコンテンツは、チェックアウトすることができない。

【0010】

ポータブルデバイス2は、パーソナルコンピュータ1から供給されたコンテンツ（すなわち、チェックアウトされたコンテンツ）を、コンテンツに関連するデータ（例えば、曲名、または利用条件など）と共に、装着されているポータブルメディア3に記憶させる。

【0011】

ポータブルメディア3は、フラッシュメモリなどの記憶媒体をその内部に有し、ポータブルデバイス2に着脱可能に構成されている。

## 【0012】

ポータブルデバイス2は、コンテンツに関連する利用条件のデータに基づいて、装着されているポータブルメディア3に記憶されているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

## 【0013】

例えば、コンテンツに関連する利用条件のデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス2は、対応するコンテンツの再生を停止する。

## 【0014】

使用者は、コンテンツを記憶したポータブルデバイス2をパーソナルコンピュータ1から取り外して、持ち歩き、ポータブルメディア3に記憶されているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

## 【0015】

ポータブルデバイス2がUSBケーブル等を介してパーソナルコンピュータ1に接続されたとき、ポータブルデバイス2とパーソナルコンピュータ1とは、相互認証の処理を実行する。この相互認証の処理は、チャレンジレスポンス方式の認証の処理である。チャレンジレスポンス方式とは、パーソナルコンピュータ1が生成するある値（チャレンジ）に対して、ポータブルデバイス2がパーソナルコンピュータ1と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。

## 【0016】

サーバ5は、所定の方式で圧縮符号化され、暗号化されたコンテンツを蓄積して、パーソナルコンピュータ1からの要求に対応して蓄積しているコンテンツを配信する。サーバ5は、鍵サーバ21、コンテンツサーバ22、およびショップサーバ23の機能を有する。

## 【0017】

鍵サーバ21は、コンテンツサーバ22がパーソナルコンピュータ1に供給したコンテンツを復号するためのコンテンツ鍵を蓄積し、パーソナルコンピュータ



1の要求に対応して、コンテンツ鍵をパーソナルコンピュータ1に供給する。コンテンツ鍵の供給の前に、鍵サーバ21とパーソナルコンピュータ1とは、相互認証の処理を実行して、鍵サーバ21は、その相互認証の処理により共有された一時鍵でコンテンツ鍵を暗号化して、パーソナルコンピュータ1に送信する。パーソナルコンピュータ1は、受信したコンテンツ鍵を共有している一時鍵で復号する。

## 【0018】

コンテンツサーバ22は、パーソナルコンピュータ1の要求に対応して、通信ネットワーク4を介して、パーソナルコンピュータ1に、コンテンツに対応する利用条件と共にコンテンツ（暗号化されている）を供給する。

## 【0019】

ショップサーバ23は、コンテンツサーバ22が供給するコンテンツに関連するデジタルデータ（コンテンツの曲名、価格などを含むコンテンツの一覧などを含む）をパーソナルコンピュータ1に提供するとともに、パーソナルコンピュータ1からのコンテンツの購入の申し込みに対応して、そのコンテンツを供給するコンテンツサーバ22のURL（Uniform Resource Locator）、およびそのコンテンツを復号するコンテンツ鍵を供給する鍵サーバ21のURLなどをパーソナルコンピュータ1に供給する。

## 【0020】

次に、図2を参照して、従来のデジタルデータ伝送システムの機能の構成について説明する。パーソナルコンピュータ1は、表示操作指示プログラム11およびLCM12に加えて、IP（Internet Protocol）通信プログラム13、ISP（Internet Service Provider）接続プログラム14、およびPHS（Personal Handyphone System）／IMT（International Mobile Telecommunication System）通信プログラム15を実行する。

## 【0021】

PHS／IMT通信プログラム15は、公衆回線網31を介して通信を行うためのプログラムである。ISP接続プログラム14は、ISP32と接続するためのプログラムである。IP通信プログラム13は、HTTP（Hypertext Tran

sport Protocol) 71 および W a p (Wireless Access Protocol) 72 などの手続を包含し、通信ネットワーク 4 を介して、鍵サーバ 21、コンテンツサーバ 22、またはショップサーバ 23 と通信するためのプログラムである。

【0022】

LCM12 は、ライセンス管理プログラム 51、鍵管理プログラム 52、コンテンツ管理プログラム 53、鍵情報受信プログラム 54、およびコンテンツ情報受信プログラム 55 から構成されている。

【0023】

ライセンス管理プログラム 51 は、コンテンツの利用条件に基づいたコンテンツの利用を管理するためのプログラムであり、利用条件管理プログラム 61、CDリッピングプログラム 62、コンバータプログラム 63、および PD 認証プログラム 64 から構成されている。

【0024】

利用条件管理プログラム 61 は、コンテンツの利用条件に基づいて、パーソナルコンピュータ 1 が記録しているコンテンツのチェックアウトなどを許可するか、または禁止するかなどの管理を実行するとともに、コンテンツのチェックアウトなどに対応して利用条件のデータを更新する。CDリッピングプログラム 62 は、パーソナルコンピュータ 1 に装着された CD からコンテンツを読み出すとともに、読み出したコンテンツに対応する利用条件を生成する。

【0025】

コンバータプログラム 63 は、コンテンツの暗号化方式、または符号化方式を変換する。PD 認証プログラム 64 は、パーソナルコンピュータ 1 に装着されているポータブルデバイス 2 を認証する。

【0026】

鍵管理プログラム 52 は、鍵サーバ 21 の認証の処理を実行して、鍵サーバ 21 からコンテンツ鍵を受信して、コンテンツに対応させてコンテンツ鍵を管理する。鍵管理プログラム 52 は、サーバ認証プログラム 65 および受信プログラム 66 から構成される。

【0027】

サーバ認証プログラム 6 5 は、後述する処理により、鍵サーバ 2 1 を認証する。受信プログラム 6 6 は、通信ネットワーク 4 を介して、鍵サーバ 2 1 からコンテンツ鍵を受信する。

【 0 0 2 8 】

コンテンツ管理プログラム 5 3 は、通信ネットワーク 4 を介して、コンテンツサーバ 2 2 からコンテンツの利用条件のデータとともにコンテンツを受信して、コンテンツの利用条件のデータとともにコンテンツを記録する。コンテンツ管理プログラム 5 3 の受信プログラム 6 7 は、コンテンツサーバ 2 2 からコンテンツの利用条件のデータおよびコンテンツを受信する。

【 0 0 2 9 】

鍵情報受信プログラム 5 4 は、ショップサーバ 2 3 から、所望のコンテンツに対応するコンテンツ鍵を供給する鍵サーバ 2 1 を特定する URL を受信する。コンテンツ情報受信プログラム 5 5 は、ショップサーバ 2 3 から、使用者が所望するコンテンツを特定するコンテンツ ID、およびそのコンテンツを供給するコンテンツサーバ 2 2 を特定する URL を受信する。

【 0 0 3 0 】

ポータブルデバイス 2 は、ライセンス管理プログラム 8 1、鍵管理プログラム 8 2、およびコンテンツ管理プログラム 8 3 を実行する。

【 0 0 3 1 】

ライセンス管理プログラム 8 1 は、コンテンツに対応する利用条件を基に、コンテンツの再生の回数などを管理する利用条件管理プログラム 9 1、パーソナルコンピュータ 1 を認証する PC 認証プログラム 9 2、およびポータブルメディア 3 を認証する PM 認証プログラム 9 3 から構成される。

【 0 0 3 2 】

鍵管理プログラム 8 2 は、パーソナルコンピュータ 1 から供給されたコンテンツ鍵を、ポータブルメディア 3 が予め記憶している保存用鍵で暗号化させ、ポータブルメディア 3 に記憶させて管理する。

【 0 0 3 3 】

コンテンツ管理プログラム 8 3 は、パーソナルコンピュータ 1 から供給された

コンテンツを、ポータブルメディア 3 に記憶させて管理する。

【 0 0 3 4 】

ポータブルメディア 3 は、ライセンス管理プログラム 1 0 1、鍵管理プログラム 1 0 2、およびコンテンツ管理プログラム 1 0 3 を実行する。

【 0 0 3 5 】

ライセンス管理プログラム 1 0 1 は、ポータブルデバイス 2 を認証する PD 認証プログラム 1 1 1 を有し、コンテンツに対応する利用条件のデータを記憶して、利用条件のデータに基づいて、コンテンツの読み出し等を制御する。鍵管理プログラム 1 0 2 は、ポータブルデバイス 2 から供給されたコンテンツ鍵を、予め記憶している保存用鍵で暗号化して記憶し、管理する。コンテンツ管理プログラム 1 0 3 は、ポータブルデバイス 2 から供給されたコンテンツを記憶して、管理する。

【 0 0 3 6 】

ショップサーバ 2 3 は、鍵情報送信プログラム 1 2 1、コンテンツ情報送信プログラム 1 2 2、閲覧プログラム 1 2 3、および IP 通信プログラム 1 2 4 を実行する。

【 0 0 3 7 】

鍵情報送信プログラム 1 2 1 は、通信ネットワーク 4 を介して、パーソナルコンピュータ 1 に、パーソナルコンピュータ 1 の使用者が所望するコンテンツに対応するコンテンツ鍵を供給する鍵サーバ 2 1 の URL を送信する。

【 0 0 3 8 】

コンテンツ情報送信プログラム 1 2 2 は、通信ネットワーク 4 を介して、パーソナルコンピュータ 1 に、パーソナルコンピュータ 1 の使用者が所望するコンテンツを供給するコンテンツサーバ 2 2 の URL を送信する。

【 0 0 3 9 】

閲覧プログラム 1 2 3 は、コンテンツをパーソナルコンピュータ 1 の使用者に視聴させる視聴プログラム 1 3 1、およびパーソナルコンピュータ 1 の使用者が所望のコンテンツを検索する検索プログラム 1 3 2 から構成されている。

【 0 0 4 0 】

I P 通信プログラム 124 は、H T T P 133 および W a p 134 などの手続を包含し、通信ネットワーク 4 を介して、パーソナルコンピュータ 1 と通信するためのプログラムである。

【0041】

鍵サーバ 21 は、認証プログラム 151、鍵配信プログラム 152、鍵保存プログラム 153、鍵生成プログラム 154、および I P 通信プログラム 155 を実行する。

【0042】

認証プログラム 151 は、パーソナルコンピュータ 1 などを認証するプログラムである。鍵配信プログラム 152 は、認証されたパーソナルコンピュータ 1 に、鍵保存プログラム 153 が保存しているコンテンツ鍵を配信するプログラムである。鍵保存プログラム 153 は、鍵生成プログラム 154 により生成されたコンテンツ鍵を保存するプログラムである。鍵生成プログラム 154 は、コンテンツに対応させてコンテンツ鍵を生成するプログラムである。

【0043】

I P 通信プログラム 155 は、H T T P 171 および W a p 172 などの手続を包含し、通信ネットワーク 4 を介して、パーソナルコンピュータ 1 などと通信するためのプログラムである。

【0044】

コンテンツサーバ 22 は、コンテンツ保存プログラム 191、コンテンツ配信プログラム 192、および I P 通信プログラム 193 を実行する。

【0045】

コンテンツ保存プログラム 191 は、コンテンツ鍵で暗号化されているコンテンツをコンテンツ I D と対応させて保存する。コンテンツ配信プログラム 192 は、パーソナルコンピュータ 1 から要求があったとき、コンテンツ保存プログラム 191 が保存している、コンテンツ I D に対応するコンテンツをパーソナルコンピュータ 1 に配信する。

【0046】

I P 通信プログラム 193 は、H T T P 201 および W a p 202 などの手続

を包含し、通信ネットワーク4を介して、パーソナルコンピュータ1と通信するためのプログラムである。

【0047】

次に、パーソナルコンピュータ1がコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする処理を図3および図4のフローチャートを参照して説明する。ステップS101において、パーソナルコンピュータ1のPHS/IMT通信プログラム15は、公衆回線網31と接続を確立する。ステップS201において、公衆回線網31の図示せぬ地上局などは、パーソナルコンピュータ1と接続を確立する。

【0048】

ステップS102において、パーソナルコンピュータ1のISP接続プログラム14は、ISP32と接続を確立する。ステップS301において、ISP32は、パーソナルコンピュータ1と接続を確立する。

【0049】

ステップS103において、パーソナルコンピュータ1のIP通信プログラム13は、ショップサーバ23とIP通信を確立する。ステップS401において、ショップサーバ23のIP通信プログラム124は、パーソナルコンピュータ1とIP通信を確立する。

【0050】

ステップS402において、ショップサーバ23の閲覧プログラム123は、通信ネットワーク4を介して、パーソナルコンピュータ1に閲覧用（コンテンツの選択用）のデジタルデータを送信する。ステップS104において、パーソナルコンピュータ1の図示せぬブラウザプログラムは、デジタルデータに対応する画像またはテキストなどを表示し、使用者に閲覧させる。また、パーソナルコンピュータ1のブラウザプログラムは、コンテンツのストリーミング再生によりコンテンツを使用者に試聴させたり、または、キーワードによりコンテンツをショップサーバ23の閲覧プログラム123に検索させ、その結果を表示する。ステップS402およびステップS104の処理は、パーソナルコンピュータ1の使用者の要求に対応して、繰り返される。

## 【0051】

ステップS105において、パーソナルコンピュータ1のブラウザプログラムは、購入依頼をショップサーバ23に送信する。ステップS403において、ショップサーバ23の閲覧プログラム123は、パーソナルコンピュータ1から送信された購入依頼を受信する。

## 【0052】

ステップS404において、ショップサーバ23のコンテンツ情報送信プログラム122は、ステップS403の処理で受信した購入依頼に対応するコンテンツを配信するコンテンツサーバ22のURLおよびコンテンツを特定するためのコンテンツIDなどを含む、コンテンツ情報を通信ネットワーク4を介してパーソナルコンピュータ1に送信する。ステップS106において、パーソナルコンピュータ1のコンテンツ情報受信プログラム55は、ショップサーバ23が送信した、コンテンツ情報を受信する。

## 【0053】

ステップS405において、ショップサーバ23の鍵情報送信プログラム121は、ステップS403の処理で受信した購入依頼に対応するコンテンツのコンテンツ鍵を配信する鍵サーバ21のURLなどの、鍵情報を通信ネットワーク4を介してパーソナルコンピュータ1に送信する。ステップS107において、パーソナルコンピュータ1の鍵情報受信プログラム54は、ショップサーバ23が送信した鍵情報を受信する。

## 【0054】

ステップS108において、パーソナルコンピュータ1のIP通信プログラム13は、ステップS106の処理で取得したコンテンツ情報に含まれるコンテンツサーバ22のURLを基に、コンテンツサーバ22とIP通信を確立する。ステップS501において、コンテンツサーバ22のIP通信プログラム193は、パーソナルコンピュータ1とIP通信を確立する。

## 【0055】

ステップS109において、パーソナルコンピュータ1のコンテンツ管理プログラム53は、ステップS106の処理で取得したコンテンツIDを、通信ネッ

トワーク 4 を介して、コンテンツサーバ 2 2 に送信する。ステップ S 5 0 2 において、コンテンツサーバ 2 2 は、パーソナルコンピュータ 1 が送信したコンテンツ ID を受信する。ステップ S 5 0 3 において、コンテンツサーバ 2 2 のコンテンツ配信プログラム 1 9 2 は、ステップ S 5 0 2 で受信したコンテンツ ID に対応するコンテンツ（暗号化されている）をコンテンツ保存プログラム 1 9 1 から読み出して、通信ネットワーク 4 を介して、パーソナルコンピュータ 1 に配信する。ステップ S 1 1 0 において、パーソナルコンピュータ 1 のコンテンツ管理プログラム 5 3 の受信プログラム 6 7 は、コンテンツサーバ 2 2 が送信したコンテンツを受信する。

## 【 0 0 5 6 】

ステップ S 1 1 1 において、パーソナルコンピュータ 1 の IP 通信プログラム 1 3 は、ステップ S 1 0 7 の処理で取得した鍵情報に含まれる鍵サーバ 2 1 の URL を基に、鍵サーバ 2 1 と IP 通信を確立する。ステップ S 6 0 1 において、鍵サーバ 2 1 の IP 通信プログラム 1 5 5 は、パーソナルコンピュータ 1 と IP 通信を確立する。

## 【 0 0 5 7 】

ステップ S 1 1 2 において、パーソナルコンピュータ 1 の鍵管理プログラム 5 2 のサーバ認証プログラム 6 5 は、鍵サーバ 2 1 を認証する。ステップ S 6 0 2 において、鍵サーバ 2 1 の認証プログラム 1 5 1 は、パーソナルコンピュータ 1 を認証する。

## 【 0 0 5 8 】

鍵サーバ 2 1 には、マスター鍵 KMS が予め記憶されており、パーソナルコンピュータ 1 には、個別鍵 KPP とパーソナルコンピュータ 1 の ID が予め記憶されている。パーソナルコンピュータ 1 には、更に、マスター鍵 KMP が予め記憶されており、鍵サーバ 2 1 にも鍵サーバ 2 1 の ID と個別鍵 KPS が記憶されている。

## 【 0 0 5 9 】

鍵サーバ 2 1 は、パーソナルコンピュータ 1 から、パーソナルコンピュータ 1 の ID の供給を受け、その ID と自分自身が有するマスター鍵 KMS にハッシュ関数を適用して、パーソナルコンピュータ 1 の個別鍵 KPP と同一の鍵を生成する。



## 【0060】

パーソナルコンピュータ1は、鍵サーバ21から、鍵サーバ21のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMPにハッシュ関数を適用して、鍵サーバ21の個別鍵KPSと同一の鍵を生成する。このようにすることで、パーソナルコンピュータ1と鍵サーバ21の両方に、共通の個別鍵が共有されることになる。これらの個別鍵を用いてさらに、一時鍵を生成する。

## 【0061】

ステップS113において、パーソナルコンピュータ1の鍵管理プログラム52は、コンテンツIDを鍵サーバ21に送信する。ステップS603において、鍵サーバ21は、パーソナルコンピュータ1が送信した、コンテンツIDを受信する。ステップS604において、鍵サーバ21の鍵配信プログラム152は、鍵保存プログラム153がコンテンツIDと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク4を介して、そのコンテンツ鍵（一時鍵により暗号化されている）をパーソナルコンピュータ1に送信する。ステップS114において、パーソナルコンピュータ1の鍵管理プログラム52の受信プログラム66は、鍵サーバ21が送信したコンテンツ鍵を受信する。鍵管理プログラム52は、受信したコンテンツ鍵を一時鍵で復号する。

## 【0062】

パーソナルコンピュータ1の使用者が、表示操作指示プログラム11に対し、受信したコンテンツのチェックアウトを指示したとき、ステップS115以降の処理が実行される。

## 【0063】

ステップS115において、パーソナルコンピュータ1のライセンス管理プログラム51のPD認証プログラム64は、ポータブルデバイス2を認証する。ステップS701において、ポータブルデバイス2のライセンス管理プログラム81のPC認証プログラム92は、パーソナルコンピュータ1を認証する。

## 【0064】

ステップS115およびステップS701におけるパーソナルコンピュータ1とポータブルデバイス2との相互認証の処理は、チャレンジレスポンス方式の認

証の処理であり、ステップS 1 1 2およびステップS 6 0 2における鍵サーバ2 1とパーソナルコンピュータ1との相互認証の処理に比較して、演算量が少ない。パーソナルコンピュータ1およびポータブルデバイス2は、それぞれ、同一の演算で、レスポンスから一時鍵を生成して、共有する。

【0 0 6 5】

ステップS 1 1 6において、パーソナルコンピュータ1のコンテンツ管理プログラム5 3は、暗号化されているコンテンツをポータブルデバイス2に配信する。ステップS 7 0 2において、ポータブルデバイス2のコンテンツ管理プログラム8 3は、パーソナルコンピュータ1が配信したコンテンツを受信して、ポータブルメディア3のコンテンツ管理プログラム1 0 3に供給する。ポータブルメディア3のコンテンツ管理プログラム1 0 3は、コンテンツを記憶する。

【0 0 6 6】

なお、ポータブルデバイス2とポータブルメディア3は、ポータブルデバイス2にポータブルメディア3が装着されたとき、相互認証する。

【0 0 6 7】

ステップS 1 1 7において、パーソナルコンピュータ1の鍵管理プログラム5 2は、ポータブルデバイス2に、ステップS 1 1 6で配信したコンテンツに対応するコンテンツ鍵（ポータブルデバイス2とポータブルメディア3とで共有する一時鍵で暗号化されている）を配信する。ステップS 7 0 3において、ポータブルデバイス2の鍵管理プログラム8 2は、パーソナルコンピュータ1が配信したコンテンツ鍵を受信して、ポータブルメディア3の鍵管理プログラム1 0 2に供給する。ポータブルメディア3の鍵管理プログラム1 0 2は、コンテンツ鍵を一時鍵で復号して、コンテンツ鍵を記憶する。

【0 0 6 8】

【発明が解決しようとする課題】

しかしながら、パーソナルコンピュータ1に比較して、演算能力または記憶容量など処理能力が小さい、例えば、携帯型端末機が、コンテンツサーバ2 2からコンテンツを直接ダウンロードし、鍵サーバ2 1からコンテンツ鍵をダウンロードしようとする、認証の処理の負荷が大きいため処理速度が遅く、実用に耐え

ない。

【 0 0 6 9 】

本発明はこのような状況に鑑みてなされたものであり、処理能力が小さくとも、不正なコンテンツの利用を防止しつつ、迅速に、コンテンツをダウンロードして利用できるようにすることを目的とする。

【 0 0 7 0 】

【課題を解決するための手段】

請求項 1 に記載の情報提供装置は、第 1 の情報処理装置を認証する第 1 の認証手段と、第 2 の情報処理装置を認証する第 2 の認証手段と、第 1 の情報処理装置からの、第 2 の情報処理装置を特定するデータおよび鍵の送信要求の受信を制御する受信制御手段と、第 2 の情報処理装置を特定するデータに基づき、第 2 の情報処理装置に鍵の送信要求を送信するとともに、第 2 の情報処理装置から鍵を受信するように通信を制御する通信制御手段と、第 1 の情報処理装置への鍵の送信を制御する送信制御手段とを含むことを特徴とする。

【 0 0 7 1 】

請求項 2 に記載の情報提供方法は、第 1 の情報処理装置を認証する第 1 の認証ステップと、第 2 の情報処理装置を認証する第 2 の認証ステップと、第 1 の情報処理装置からの、第 2 の情報処理装置を特定するデータおよび鍵の送信要求の受信を制御する受信制御ステップと、第 2 の情報処理装置を特定するデータに基づき、第 2 の情報処理装置に鍵の送信要求を送信するとともに、第 2 の情報処理装置から鍵を受信するように通信を制御する通信制御ステップと、第 1 の情報処理装置への鍵の送信を制御する送信制御ステップとを含むことを特徴とする。

【 0 0 7 2 】

請求項 3 に記載のプログラム格納媒体のプログラムは、第 1 の情報処理装置を認証する第 1 の認証ステップと、第 2 の情報処理装置を認証する第 2 の認証ステップと、第 1 の情報処理装置からの、第 2 の情報処理装置を特定するデータおよび鍵の送信要求の受信を制御する受信制御ステップと、第 2 の情報処理装置を特定するデータに基づき、第 2 の情報処理装置に鍵の送信要求を送信するとともに、第 2 の情報処理装置から鍵を受信するように通信を制御する通信制御ステップ

と、第1の情報処理装置への鍵の送信を制御する送信制御ステップとを含むことを特徴とする。

【0073】

請求項4に記載の情報処理装置は、第1の情報提供装置を認証する認証手段と、第1の情報提供装置への、鍵を提供する第2の情報提供装置を特定するデータおよび鍵の送信要求の送信を制御する送信制御手段と、第2の情報提供装置から第1の情報提供装置が提供を受け、送信した鍵の受信を制御する受信制御手段とを含むことを特徴とする。

【0074】

請求項5に記載の情報処理方法は、第1の情報提供装置を認証する認証ステップと、第1の情報提供装置への、鍵を提供する第2の情報提供装置を特定するデータおよび鍵の送信要求の送信を制御する送信制御ステップと、第2の情報提供装置から第1の情報提供装置が提供を受け、送信した鍵の受信を制御する受信制御ステップとを含むことを特徴とする。

【0075】

請求項6に記載のプログラム格納媒体のプログラムは、第1の情報提供装置を認証する認証ステップと、第1の情報提供装置への、鍵を提供する第2の情報提供装置を特定するデータおよび鍵の送信要求の送信を制御する送信制御ステップと、第2の情報提供装置から第1の情報提供装置が提供を受け、送信した鍵の受信を制御する受信制御ステップとを含むことを特徴とする。

【0076】

請求項1に記載の情報提供装置、請求項2に記載の情報提供方法、および請求項3に記載のプログラム格納媒体においては、第1の情報処理装置が認証され、第2の情報処理装置が認証され、第1の情報処理装置からの、第2の情報処理装置を特定するデータおよび鍵の送信要求の受信が制御され、第2の情報処理装置を特定するデータに基づき、第2の情報処理装置に鍵の送信要求を送信するとともに、第2の情報処理装置から鍵を受信するように通信が制御され、第1の情報処理装置への鍵の送信が制御される。

【0077】

請求項４に記載の情報処理装置、請求項５に記載の情報処理方法、および請求項６に記載のプログラム格納媒体においては、第１の情報提供装置が認証され、第１の情報提供装置への、鍵を提供する第２の情報提供装置を特定するデータおよび鍵の送信要求の送信が制御され、第２の情報提供装置から第１の情報提供装置が提供を受け、送信した鍵の受信が制御される。

【００７８】

【発明の実施の形態】

図５は、本発明に係るデジタルデータ伝送システムの一実施の形態を示す図である。図１で説明した構成の場合と同一の部分には、図１の場合と同一の番号を付してあり、その説明は省略する。

【００７９】

電話機一体型端末機５０１は、ポータブルメディア３－１を装着可能に構成され、無線により、通信ネットワーク４に接続される。電話機一体型端末機５０１は、通信ネットワーク４を介して、コンテンツサーバ２２から受信したコンテンツ（所定の方式で圧縮され、暗号化されている）を、利用条件のデータ等と共にダウンロードして、コンテンツおよびその利用条件のデータを装着されているポータブルメディア３－１に記憶させる。

【００８０】

電話機一体型端末機５０１は、コンテンツに関連する利用条件のデータに基づいて、装着されているポータブルメディア３－１に記憶されているコンテンツを再生し、図示せぬヘッドフォンまたはスピーカなどに出力する。使用者は、電話機一体型端末機５０１を持ち歩きながら、所望の場所で所望のコンテンツをダウンロードして、そのコンテンツをポータブルメディア３に記憶させることができる。使用者は、電話機一体型端末機５０１に、ポータブルメディア３に記憶されているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【００８１】

電話機一体型端末機５０１の表示操作指示プログラム５１１は、コンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、

ダウンロードの指示などを入力して、クライアント用LCM512にその指示に対応した処理を実行させる。電話機一体型端末機501のクライアント用LCM512は、認証サーバ503のサーバ用LCM514と協同して、利用条件データおよびコンテンツ等をダウンロードする一連の処理（後述する）を実行する。

【0082】

電話機一体型端末機501のクライアント用LCM512は、コンテンツの不正な2次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【0083】

クライアント用LCM512は、電話機一体型端末機501に装着されているポータブルメディア3-1が正当であるかの認証を行い、安全な方法でサーバ5が指定した利用条件のデータをコンテンツ（暗号化されている）に付加して、ポータブルメディア3-1にコンテンツを記録させる。コンテンツの移動の処理などに伴い、クライアント用LCM512は、必要な鍵を生成して、鍵を管理し、または接続されているポータブルメディア3-1との通信を制御する。

【0084】

パーソナルコンピュータ502は、通信ネットワーク4に接続されている。パーソナルコンピュータ502は、コンテンツサーバ22から受信した、またはCDから読み取ったコンテンツを、所定の圧縮の方式に変換するとともにDESなどの暗号化方式で暗号化して記録する。パーソナルコンピュータ502は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

【0085】

パーソナルコンピュータ502の表示操作指示プログラム11は、コンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、ダウンロード、またはチェックアウトの指示などを入力して、LCM513にその指示に対応したダウンロード、またはチェックアウトなどの処理を実行させ

る。

【 0 0 8 6 】

パーソナルコンピュータ 5 0 2 の L C M 5 1 3 は、コンテンツの不正な 2 次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【 0 0 8 7 】

L C M 5 1 3 は、パーソナルコンピュータ 5 0 2 に接続されたポータブルデバイス 2 が正当であるかの認証を行い、安全な方法でコンテンツの移動の処理などを実行する。コンテンツの移動の処理などに伴い、L C M 5 1 3 は、必要な鍵を生成して、鍵を管理し、コンテンツを暗号化し、または接続されている機器との通信を制御する。

【 0 0 8 8 】

また、L C M 5 1 3 は、ポータブルデバイス 2 の正当性をチェックする。ポータブルデバイス 2 は、ポータブルメディア 3 - 2 が装着されたとき、ポータブルメディア 3 - 2 の正当性をチェックする。ポータブルデバイス 2 およびポータブルメディア 3 - 2 が正当である場合、L C M 5 1 3 は、サーバ 5 が指定した利用条件のデータをコンテンツ（暗号化されている）に付加して、ポータブルメディア 3 - 2 にコンテンツをチェックアウトする。ポータブルデバイス 2 は、パーソナルコンピュータ 5 0 2 からチェックアウトされたコンテンツを、コンテンツに関連するデータと共に、装着されているポータブルメディア 3 - 2 に記憶させる。

【 0 0 8 9 】

認証サーバ 5 0 3 を利用できるとき、パーソナルコンピュータ 5 0 2 の P C 用 L C M 5 2 1 （L C M 5 1 3 の一部または全部の機能から構成される）は、認証サーバ 5 0 3 のサーバ用 L C M 5 1 4 と協同して、利用条件データおよびコンテンツ等をダウンロードする一連の処理を実行する。

【 0 0 9 0 】

認証サーバ503を利用できないとき、パーソナルコンピュータ502のLCM513は、LCM12と同様の鍵サーバ21との認証の処理等を実行して、利用条件データおよびコンテンツ等をダウンロードする。

【0091】

認証サーバ503は、サーバ用LCM514を実行して、相互認証した電話機一体型端末機501または相互認証したパーソナルコンピュータ502の要求に対応して、鍵サーバ21との認証の処理を実行する。認証サーバ503は、鍵サーバ21との相互認証の処理の後、鍵サーバ21からコンテンツ鍵を受信して、受信したコンテンツ鍵を電話機一体型端末機501またはパーソナルコンピュータ502に供給する。

【0092】

電話機一体型端末機501またはパーソナルコンピュータ502は、鍵サーバ21との認証の処理の実行を必要とせず、鍵サーバ21との認証の処理に比較してより処理の負荷の小さい認証サーバ503との認証の処理を実行するだけで、コンテンツ鍵を取得することができる。

【0093】

図6は、電話機一体型端末機501の構成を説明する図である。CPU (Central Processing Unit) 601は、ROM (Read-only Memory) 602またはRAM (Random-Access Memory) 603に格納されている各種プログラムを実際に実行する。ROM602は、EEPROM (Electrically Erasable Programmable Read-Only Memory) またはフラッシュメモリなどで構成され、一般的には、CPU601が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM603は、SRAM (Static RAM) など構成され、CPU601の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。

【0094】

入力部605は、入力キーまたはマイクロフォンなどで構成され、CPU601に各種の指令を入力するとき、または音声などを入力するとき、使用者により操作される。表示部606は、液晶表示装置などから成り、各種情報をテキストやイメージで表示する。



## 【0095】

音声再生部607は、通信部608から供給された通話相手の音声のデータ、またはインターフェース609から供給されたポータブルメディア3-1に記憶されているコンテンツを再生して、音声を出力する。

## 【0096】

通信部608は、公衆回線網31と接続し、CPU601から供給されたデータ（例えば、コンテンツの送信要求など）または入力部605から供給された使用者の音声のデータを、所定の方式のパケットに格納して、公衆回線網31を介して、送信する。また、通信部608は、公衆回線網31を介して、受信したパケットに格納されているデータ（例えば、コンテンツなど）または通話相手の音声のデータをCPU601、RAM603、音声再生部607、またはインターフェース609に出力する。

## 【0097】

インターフェース609は、CPU601、RAM603、または通信部608から供給されたデータを装着されているポータブルメディア3-1に記憶させるとともに、装着されているポータブルメディア3-1からコンテンツなどのデータを読み出して、CPU601、RAM603、または音声再生部607に供給する。

## 【0098】

インターフェース610は、外付けのドライブ631が接続される。ドライブ631は、装着されている磁気ディスク641、光ディスク642（CD-ROMを含む）、光磁気ディスク643、または半導体メモリ644に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース610、およびバス604を介して接続されているROM602またはRAM603に供給する。

## 【0099】

CPU601乃至インターフェース610は、バス604により相互に接続されている。

## 【0100】

図7は、認証サーバ503の構成を説明する図である。CPU651は、各種ア

アプリケーションプログラム（詳細については後述する）や、OS (Operating System)を実際に実行する。ROM 652は、一般的には、CPU 651が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM 653は、CPU 651の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス 654により相互に接続されている。

#### 【0101】

ホストバス 654は、ブリッジ 655を介して、PCI (Peripheral Component Interconnect/Interface)バスなどの外部バス 656に接続されている。

#### 【0102】

キーボード 658は、CPU 651に各種の指令を入力するとき、使用者により操作される。ポインティングデバイス 659は、ディスプレイ 660の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ 660は、液晶表示装置またはCRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。HDD (Hard Disk Drive) 661は、ハードディスクを駆動し、それらにCPU 651によって実行するプログラムや情報を記録または再生させる。

#### 【0103】

ドライブ 662は、装着されている磁気ディスク 681、光ディスク 682、光磁気ディスク 683、または半導体メモリ 684に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース 657、外部バス 656、ブリッジ 655、およびホストバス 654を介して接続されているRAM 653に供給する。

#### 【0104】

これらのキーボード 658乃至ドライブ 662は、インターフェース 657に接続されており、インターフェース 657は、外部バス 656、ブリッジ 655、およびホストバス 654を介してCPU 651に接続されている。

#### 【0105】

通信部 663は、通信ネットワーク 4が接続され、CPU 651、またはHDD 66

1から供給されたデータ（例えば、コンテンツ鍵など）を、所定の方式のパケットに格納して、通信ネットワーク4を介して、送信するとともに、通信ネットワーク4を介して、受信したパケットに格納されているデータ（例えば、コンテンツIDなど）をCPU651、RAM653、またはHDD661に出力する。

【0106】

通信部663は、外部バス656、ブリッジ655、およびホストバス654を介してCPU651に接続されている。

【0107】

次に、図8を参照して、本願のデジタルデータ伝送システムの機能の構成について説明する。図2で説明した構成の場合と同一の部分には、図2の場合と同一の番号を付してあり、その説明は省略する。

【0108】

電話機一体型端末機501は、表示操作指示プログラム511、クライアント用LCM512、IP通信プログラム701、ISP接続プログラム702、およびPHS/IMT通信プログラム703を実行する。

【0109】

PHS/IMT通信プログラム703は、公衆回線網31を介して通信を行うためのプログラムである。ISP接続プログラム702は、ISP32と接続するためのプログラムである。IP通信プログラム701は、HTTP731およびWap732などの手続を包含し、通信ネットワーク4を介して、鍵サーバ21、コンテンツサーバ22、ショップサーバ23、または認証サーバ503などと通信するためのプログラムである。

【0110】

クライアント用LCM512は、ライセンス管理プログラム711、鍵管理プログラム712、コンテンツ管理プログラム713、鍵情報受信プログラム714、およびコンテンツ情報受信プログラム715などから構成されている。

【0111】

ライセンス管理プログラム711は、コンテンツの利用条件に基づいたコンテンツの利用を管理するためのプログラムであり、利用条件管理プログラム721

、サーバ認証プログラム 7 2 2、および PM 認証プログラム 7 2 3 から構成されている。

#### 【 0 1 1 2 】

利用条件管理プログラム 7 2 1 は、コンテンツの利用条件に基づいて、ポータブルメディア 3 - 1 が記憶しているコンテンツの再生などを許可するか、または禁止するかなどの管理を実行するとともに、ポータブルメディア 3 - 1 が記憶しているコンテンツの再生などに対応して、ポータブルメディア 3 - 1 に、ポータブルメディア 3 - 1 が記憶している利用条件のデータを更新させる。サーバ認証プログラム 7 2 2 は、通信ネットワーク 4 を介して、認証サーバ 5 0 3 を認証する。PM 認証プログラム 7 2 3 は、ポータブルメディア 3 - 1 が電話機一体型端末機 5 0 1 に装着されたとき、ポータブルメディア 3 - 1 を認証する。

#### 【 0 1 1 3 】

鍵管理プログラム 7 1 2 は、認証サーバ 5 0 3 からコンテンツ鍵を受信して、コンテンツに対応させて、コンテンツ鍵をポータブルメディア 3 - 1 に記憶させて、管理する。鍵管理プログラム 7 1 2 は、認証サーバ 5 0 3 からコンテンツ鍵を受信する受信プログラム 7 2 4 などを含む。

#### 【 0 1 1 4 】

コンテンツ管理プログラム 7 1 3 は、コンテンツサーバ 2 2 からコンテンツの利用条件とともにコンテンツ（暗号化されている）を受信して、コンテンツの利用条件とともにコンテンツをポータブルメディア 3 - 1 に記憶させる。コンテンツ管理プログラム 7 1 3 の受信プログラム 7 2 5 は、コンテンツサーバ 2 2 からコンテンツの利用条件およびコンテンツを受信する。

#### 【 0 1 1 5 】

鍵情報受信プログラム 7 1 4 は、ショップサーバ 2 3 から、コンテンツに対応するコンテンツ鍵を供給する鍵サーバ 2 1 を特定する URL を受信する。コンテンツ情報受信プログラム 7 1 5 は、ショップサーバ 2 3 から、所望のコンテンツを特定するコンテンツ ID、および所望のコンテンツを供給するコンテンツサーバ 2 2 を特定する URL を受信する。

#### 【 0 1 1 6 】

認証サーバ503は、サーバ用LCM514、およびIP通信プログラム741を実行する。

【0117】

サーバ用LCM514は、ライセンス管理プログラム751、および鍵管理プログラム752などを含む。

【0118】

ライセンス管理プログラム751は、更に、鍵サーバ21を認証するサーバ認証プログラム761、および電話機一体型端末機501を認証するPD認証プログラム762などを含む。

【0119】

鍵管理プログラム752は、更に、通信ネットワーク4を介して、鍵サーバ21からコンテンツ鍵を受信する鍵受信プログラム763、および通信ネットワーク4を介して、受信したコンテンツ鍵を電話機一体型端末機501に配信する鍵配信プログラム764などを含む。

【0120】

IP通信プログラム741は、HTTP765およびWap766などの手続を包含し、通信ネットワーク4を介して、鍵サーバ21または電話機一体型端末機501と通信するためのプログラムである。

【0121】

次に、電話機一体型端末機501がコンテンツをダウンロードする処理を図9および図10のフローチャートを参照して説明する。ステップS1001において、電話機一体型端末機501のPHS/IMT通信プログラム703は、公衆回線網31と接続を確立する。ステップS1101において、公衆回線網31の図示せぬ地上局などは、電話機一体型端末機501と接続を確立する。

【0122】

ステップS1002において、電話機一体型端末機501のISP接続プログラム702は、電話機一体型端末機501と公衆回線網31との接続を介して、ISP32と接続を確立する。ステップS1201において、ISP32は、電話機一体型端末機501と公衆回線網31との接続を介して、電話機一体型端末

機 5 0 1 と接続を確立する。

【 0 1 2 3 】

以降の電話機一体型端末機 5 0 1 と、鍵サーバ 2 1、コンテンツサーバ 2 2、ショップサーバ 2 3、または認証サーバ 5 0 3 との処理は、電話機一体型端末機 5 0 1 と I S P 3 2 との接続を介して実行される。

【 0 1 2 4 】

ステップ S 1 0 0 3 において、電話機一体型端末機 5 0 1 の I P 通信プログラム 7 0 1 は、ショップサーバ 2 3 と I P 通信を確立する。ステップ S 1 3 0 1 において、ショップサーバ 2 3 の I P 通信プログラム 1 2 4 は、電話機一体型端末機 5 0 1 と I P 通信を確立する。

【 0 1 2 5 】

ステップ S 1 3 0 2 において、ショップサーバ 2 3 の閲覧プログラム 1 2 3 は、通信ネットワーク 4 を介して、電話機一体型端末機 5 0 1 に閲覧用（コンテンツの選択用）のデジタルデータを送信する。ステップ S 1 0 0 4 において、電話機一体型端末機 5 0 1 の図示せぬブラウザプログラムは、受信したデジタルデータに対応するテキストまたは画像を表示部 6 0 6 に表示させ、使用者に閲覧させる。また、電話機一体型端末機 5 0 1 のブラウザプログラムは、コンテンツのストリーミング再生により、コンテンツを音声再生部 6 0 7 に再生させて、使用者に試聴させたり、または、キーワードにより所望のコンテンツをショップサーバ 2 3 の閲覧プログラム 1 2 3 に検索させ、その結果を表示部 6 0 6 に表示させる。

【 0 1 2 6 】

ステップ S 1 3 0 2 およびステップ S 1 0 0 4 の処理は、電話機一体型端末機 5 0 1 の使用者の要求に対応して、例えば、使用者が購入するコンテンツを決定するまで繰り返される。

【 0 1 2 7 】

ステップ S 1 0 0 5 において、電話機一体型端末機 5 0 1 のブラウザプログラムは、通信ネットワーク 4 を介して、購入依頼をショップサーバ 2 3 に送信する。ステップ S 1 3 0 3 において、ショップサーバ 2 3 の閲覧プログラム 1 2 3 は

、電話機一体型端末機 5 0 1 から送信された購入依頼を受信する。

【 0 1 2 8 】

ステップ S 1 3 0 4 において、ショップサーバ 2 3 のコンテンツ情報送信プログラム 1 2 2 は、ステップ S 1 3 0 3 の処理で受信した購入依頼に対応して、コンテンツを配信するコンテンツサーバ 2 2 の URL、およびコンテンツを特定するためのコンテンツ ID などを含む、コンテンツ情報を、通信ネットワーク 4 を介して、電話機一体型端末機 5 0 1 に送信する。ステップ S 1 0 0 6 において、電話機一体型端末機 5 0 1 のコンテンツ情報受信プログラム 7 1 5 は、ショップサーバ 2 3 が送信した、コンテンツ情報を受信する。

【 0 1 2 9 】

ステップ S 1 3 0 5 において、ショップサーバ 2 3 の鍵情報送信プログラム 1 2 1 は、ステップ S 1 3 0 3 の処理で受信した購入依頼に対応するコンテンツのコンテンツ鍵を配信する鍵サーバ 2 1 の URL などの、鍵情報を通信ネットワーク 4 を介して、電話機一体型端末機 5 0 1 に送信する。ステップ S 1 0 0 7 において、電話機一体型端末機 5 0 1 の鍵情報受信プログラム 7 1 4 は、ショップサーバ 2 3 が送信した、鍵情報を受信する。

【 0 1 3 0 】

ステップ S 1 0 0 8 において、電話機一体型端末機 5 0 1 の IP 通信プログラム 7 0 1 は、ステップ S 1 0 0 6 の処理で取得したコンテンツ情報に含まれるコンテンツサーバ 2 2 の URL を基に、コンテンツサーバ 2 2 と IP 通信を確立する。ステップ S 1 4 0 1 において、コンテンツサーバ 2 2 の IP 通信プログラム 1 9 3 は、電話機一体型端末機 5 0 1 と IP 通信を確立する。

【 0 1 3 1 】

ステップ S 1 0 0 9 において、電話機一体型端末機 5 0 1 のコンテンツ管理プログラム 7 1 3 は、ステップ S 1 0 0 6 の処理で取得したコンテンツ ID を、通信ネットワーク 4 を介して、コンテンツサーバ 2 2 に送信する。ステップ S 1 4 0 2 において、コンテンツサーバ 2 2 は、電話機一体型端末機 5 0 1 が送信したコンテンツ ID を受信する。ステップ S 1 4 0 3 において、コンテンツサーバ 2 2 のコンテンツ配信プログラム 1 9 2 は、ステップ S 1 4 0 2 で受信したコンテ

ンツIDに対応するコンテンツ（暗号化されている）を、コンテンツ保存プログラム191から読み出して、通信ネットワーク4を介して、電話機一体型端末機501に配信する。

【0132】

ステップS1010において、電話機一体型端末機501のコンテンツ管理プログラム713の受信プログラム725は、コンテンツサーバ22が送信したコンテンツを受信する。コンテンツ管理プログラム713は、受信したコンテンツを、インターフェース609を介して、ポータブルメディア3-1に供給して、コンテンツ管理プログラム103に、コンテンツを記憶させる。

【0133】

ステップS1011において、電話機一体型端末機501のIP通信プログラム701は、ステップS1007の処理で取得した鍵情報に含まれる鍵サーバ21のURLを基に、認証サーバ503とIP通信を確立する。ステップS1501において、認証サーバ503のIP通信プログラム741は、電話機一体型端末機501とIP通信を確立する。

【0134】

ステップS1012において、電話機一体型端末機501のライセンス管理プログラム711のサーバ認証プログラム722は、認証サーバ503を認証する。ステップS1502において、認証サーバ503のライセンス管理プログラム751のPD認証プログラム762は、電話機一体型端末機501を認証する。

【0135】

ステップS1012およびステップS1502における電話機一体型端末機501と認証サーバ503との相互認証の処理は、チャレンジレスポンス方式の認証の処理であり、ステップS112およびステップS602における鍵サーバ21とパーソナルコンピュータ1との相互認証の処理に比較して、演算量が少なく、少ない演算能力、または記憶容量でも、迅速に実行することができる。電話機一体型端末機501および認証サーバ503は、それぞれ、同一の演算で、レスポンスから一時鍵を生成して、共有する。

【0136】



ステップ S 1 0 1 2 またはステップ S 1 5 0 2 における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、電話機一体型端末機 5 0 1 がコンテンツをダウンロードする処理は、コンテンツ鍵が電話機一体型端末機 5 0 1 にダウンロードされずに終了するので、電話機一体型端末機 5 0 1 は、コンテンツを利用することができない。

## 【 0 1 3 7 】

ステップ S 1 0 1 3 において、電話機一体型端末機 5 0 1 の鍵管理プログラム 7 1 2 は、コンテンツ ID を認証サーバ 5 0 3 に送信する。ステップ S 1 5 0 3 において、認証サーバ 5 0 3 は、電話機一体型端末機 5 0 1 が送信したコンテンツ ID を受信する。ステップ S 1 0 1 4 において、電話機一体型端末機 5 0 1 の鍵管理プログラム 7 1 2 は、ステップ S 1 0 0 7 の処理で受信した鍵情報を認証サーバ 5 0 3 に送信する。ステップ S 1 5 0 4 において、認証サーバ 5 0 3 は、電話機一体型端末機 5 0 1 が送信した、鍵情報を受信する。

## 【 0 1 3 8 】

ステップ S 1 5 0 5 において、認証サーバ 5 0 3 の IP 通信プログラム 7 4 1 は、鍵サーバ 2 1 と IP 通信を確立する。ステップ S 1 6 0 1 において、鍵サーバ 2 1 の IP 通信プログラム 1 5 5 は、認証サーバ 5 0 3 と IP 通信を確立する。

## 【 0 1 3 9 】

ステップ S 1 0 1 6 において、認証サーバ 5 0 3 のライセンス管理プログラム 7 5 1 のサーバ認証プログラム 7 6 1 は、鍵サーバ 2 1 を認証する。ステップ S 1 6 0 2 において、鍵サーバ 2 1 の認証プログラム 1 5 1 は、認証サーバ 5 0 3 を認証する。

## 【 0 1 4 0 】

例えば、鍵サーバ 2 1 には、マスター鍵 KMSS が予め記憶されており、認証サーバ 5 0 3 には、個別鍵 KPCC と認証サーバ 5 0 3 の ID が予め記憶されている。認証サーバ 5 0 3 には、更に、マスター鍵 KMCC が予め記憶されており、鍵サーバ 2 1 にも鍵サーバ 2 1 の ID と個別鍵 KPSS が記憶されている。

## 【 0 1 4 1 】

鍵サーバ21は、認証サーバ503から、認証サーバ503のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMSSにハッシュ関数を適用して、認証サーバ503の個別鍵KPCCと同一の鍵を生成する。

【0142】

認証サーバ503は、鍵サーバ21から、鍵サーバ21のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMCCにハッシュ関数を適用して、鍵サーバ21の個別鍵KPSSと同一の鍵を生成する。このようにすることで、認証サーバ503と鍵サーバ21の両方に、共通の個別鍵が共有されることになる。これらの個別鍵を用いてさらに、一時的な一時鍵を生成する。

【0143】

ステップS1506またはステップS1602における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、電話機一体型端末機501がコンテンツをダウンロードする処理は、コンテンツ鍵が電話機一体型端末機501にダウンロードされずに終了するので、電話機一体型端末機501は、コンテンツを利用することができない。

【0144】

ステップS1507において、認証サーバ503の鍵管理プログラム752は、ステップS1503の処理で取得したコンテンツIDを鍵サーバ21に送信する。ステップS1603において、鍵サーバ21は、認証サーバ503が送信したコンテンツIDを受信する。ステップS1604において、鍵サーバ21の鍵配信プログラム152は、鍵保存プログラム153がコンテンツIDと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク4を介して、そのコンテンツ鍵（鍵サーバ21と認証サーバ503とで共有する一時鍵で暗号化されている）を認証サーバ503に送信する。ステップS1508において、認証サーバ503の鍵管理プログラム752の鍵受信プログラム763は、鍵サーバ21が送信したコンテンツ鍵を受信する。

【0145】

ステップS1509において、認証サーバ503の鍵管理プログラム752の鍵配信プログラム764は、ステップS1508の処理で受信したコンテンツ鍵

を、鍵サーバ21と認証サーバ503とで共有する一時鍵で復号し、電話機一体型端末機501と認証サーバ503で共有する一時鍵で暗号化して、通信ネットワーク4を介して、暗号化されているコンテンツ鍵を電話機一体型端末機501に送信する。ステップS1015において、電話機一体型端末機501の鍵管理プログラム712の受信プログラム724は、認証サーバ503が送信したコンテンツ鍵を受信する。鍵管理プログラム712は、コンテンツ鍵を電話機一体型端末機501と認証サーバ503で共有する一時鍵で復号して、ポータブルメディア3の鍵管理プログラム102に供給し、鍵管理プログラム102に、コンテンツ鍵を記憶させる。

## 【0146】

ステップS1012およびステップS1502における電話機一体型端末機501と認証サーバ503との相互認証の処理は、電話機一体型端末機501と鍵サーバ21が相互認証する場合の処理に比較して、演算量が少なく、高い演算能力、または大きな記憶容量などを必要としない。従って、相互認証を実行することにより不正なコンテンツの利用を防止しつつ、電話機一体型端末機501は、処理能力が小さくとも、迅速に、コンテンツをダウンロードして利用できる。

## 【0147】

さらに、電話機一体型端末機501は、コンテンツのダウンロードと同時に、コンテンツをポータブルメディア3に記憶させることができるので、使用者は、電話機一体型端末機501に対してチェックアウトなどの操作を指示する必要がなく、迅速に、コンテンツを利用することができる。

## 【0148】

また、サーバ用LCM514の更新（例えば、バージョンアップ）は、認証サーバ503の管理者が一元的に迅速に行うことができる。さらに、クライアント用LCM512は、従来のLCM12に比較して、小さなプログラムとなるので（例えば、サーバ認証プログラム722は、従来のサーバ認証プログラム65に比較して小さくインプリメントできる。）、電話機一体型端末機501は、クライアント用LCM512を更新する処理を迅速に行うことができる。

## 【0149】

なお、認証サーバ503を利用することができるとき、パーソナルコンピュータ502のPC用LCM521は、上述した電話機一体型端末機501のクライアント用LCM512と同様の処理を実行する。認証サーバ503を利用することができないとき、パーソナルコンピュータ502のLCM513は、従来のLCM12と同様の処理を実行する。

【0150】

また、コンテンツは、楽音のデータであると説明したが、楽音のデータに限らず、静止画像のデータ、動画像のデータ、テキストのデータ、またはプログラムなどでもよい。

【0151】

なお、電話機一体型端末機501またはパーソナルコンピュータ502が、コンテンツをダウンロードすると説明したが、電話機一体型端末機501またはパーソナルコンピュータ502に限らず、携帯電話機、PDA (Personal Digital Assistant)、通信機能付き撮像機能付きデジタルビデオカセットレコーダ、通信機能付き電子手帳装置、または携帯型パーソナルコンピュータなどがコンテンツをダウンロードするようにしてもよい。

【0152】

また、電話機一体型端末機501は、PHSまたはIMTにより通信すると説明したが、PHSまたはIMTに限らず、W-CDMA (Code Division Multiple Access)、衛星通信、衛星放送、PSTN (Public Switched telephone network)、xD SL (x Digital Subscriber Line)、ISDN (Integrated Services Digital Network)、またはプライベートネットワークなどで通信するようにしてもよい。

【0153】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

## 【0154】

コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図6または図7に示すように、磁気ディスク641若しくは磁気ディスク681（いずれもフロッピーディスクを含む）、光ディスク642若しくは光ディスク682（いずれも、CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク643若しくは光磁気ディスク683（いずれもMD(Mini-Disc)を含む）、若しくは半導体メモリ644若しくは半導体メモリ684などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM602若しくはROM652や、HDD661などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じて通信部608または通信部663を介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

## 【0155】

なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

## 【0156】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

## 【0157】

## 【発明の効果】

請求項1に記載の情報提供装置、請求項2に記載の情報提供方法、および請求項3に記載のプログラム格納媒体によれば、第1の情報処理装置が認証され、第2の情報処理装置が認証され、第1の情報処理装置からの、第2の情報処理装置を特定するデータおよび鍵の送信要求の受信が制御され、第2の情報処理装置を特定するデータに基づき、第2の情報処理装置に鍵の送信要求を送信するとともに、第2の情報処理装置から鍵を受信するように通信が制御され、第1の情報処

理装置への鍵の送信が制御されるようにしたので、第1の情報処理装置は、処理能力が小さくとも、不正なコンテンツの利用を防止しつつ、迅速に、コンテンツをダウンロードして利用できるようになる。

【0158】

請求項4に記載の情報処理装置、請求項5に記載の情報処理方法、および請求項6に記載のプログラム格納媒体においては、第1の情報提供装置が認証され、第1の情報提供装置への、鍵を提供する第2の情報提供装置を特定するデータおよび鍵の送信要求の送信が制御され、第2の情報提供装置から第1の情報提供装置が提供を受け、送信した鍵の受信が制御されるようにしたので、処理能力が小さくとも、不正なコンテンツの利用を防止しつつ、迅速に、コンテンツをダウンロードして利用できるようになる。

【図面の簡単な説明】

【図1】

従来のデジタルデータ伝送システムの構成を示す図である。

【図2】

従来のデジタルデータ伝送システムの機能の構成を示す図である。

【図3】

パーソナルコンピュータ1がコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする処理を説明するフローチャートである。

【図4】

パーソナルコンピュータ1がコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする処理を説明するフローチャートである。

【図5】

本発明に係るデジタルデータ伝送システムの一実施の形態を示す図である。

【図6】

電話機一体型端末機501の構成を説明する図である。

【図7】

認証サーバ503の構成を説明する図である。

【図8】

本願のデジタルデータ伝送システムの機能の構成を説明する図である。

【図 9】

電話機一体型端末機 5 0 1 がコンテンツをダウンロードする処理を説明するフローチャートである。

【図 1 0】

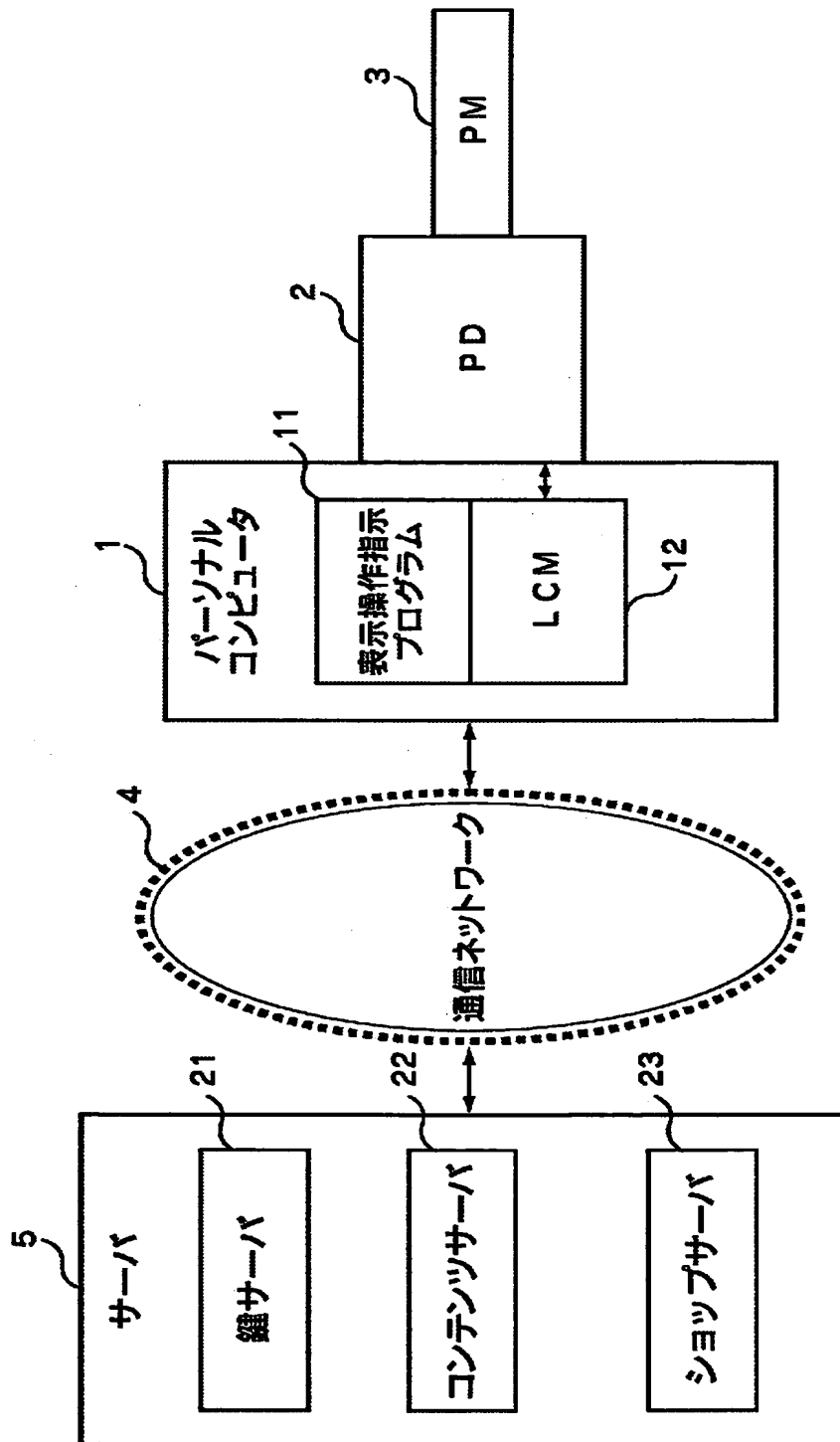
電話機一体型端末機 5 0 1 がコンテンツをダウンロードする処理を説明するフローチャートである。

【符号の説明】

5 0 1 電話機一体型端末機, 5 0 3 認証サーバ, 5 1 1 表示操作指示プログラム, 5 1 2 クライアント用 LCM, 5 1 4 サーバ用 LCM, 6 0 1 CPU, 6 0 2 ROM, 6 0 3 RAM, 6 0 8 通信部, 6 4 1 磁気ディスク, 6 4 2 光ディスク, 6 4 3 光磁気ディスク, 6 4 4 半導体メモリ, 6 5 1 CPU, 6 5 2 ROM, 6 5 3 RAM, 6 6 3 通信部, 6 8 1 磁気ディスク, 6 8 2 光ディスク, 6 8 3 光磁気ディスク, 6 8 4 半導体メモリ

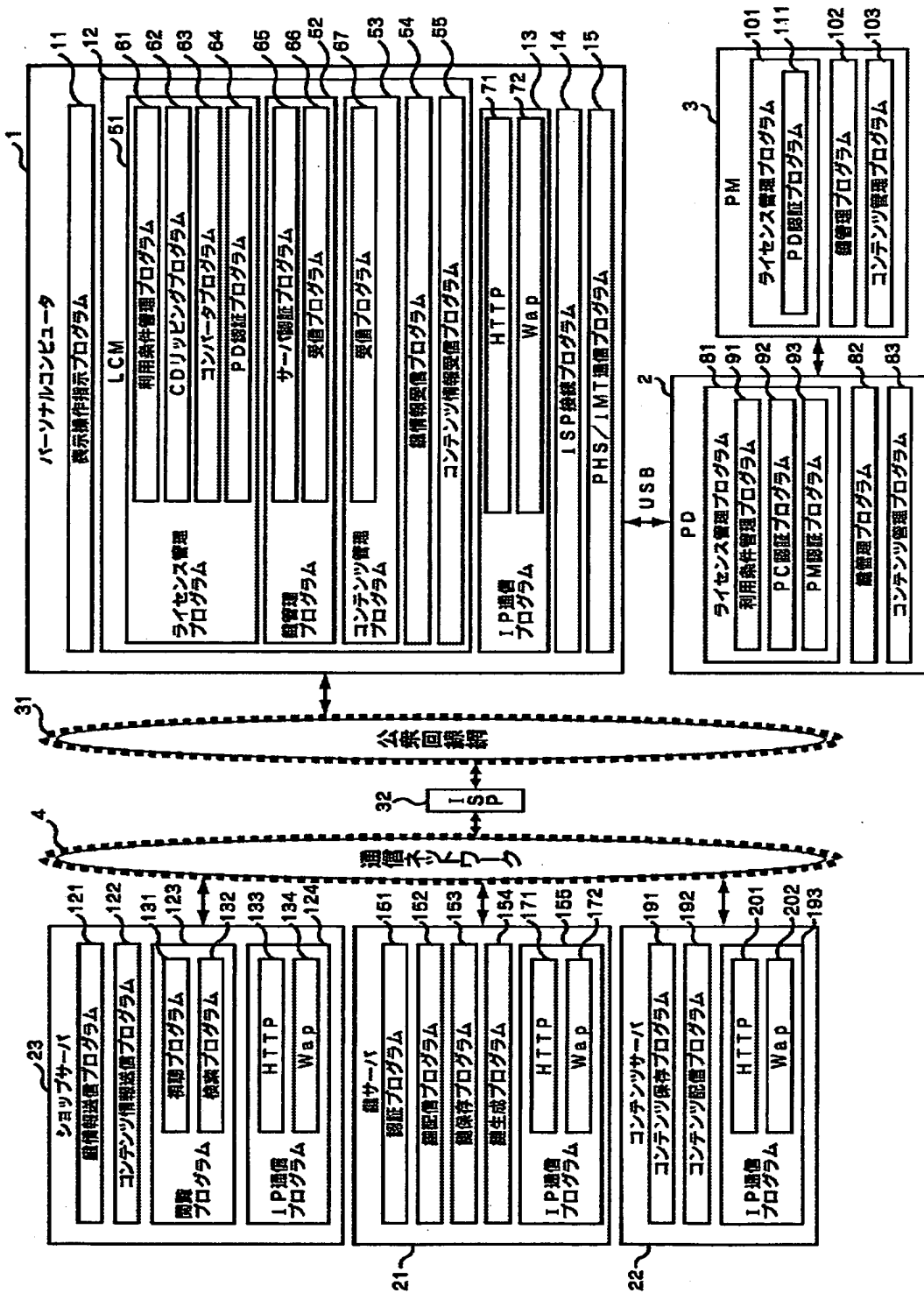
【書類名】 図面

【図 1】



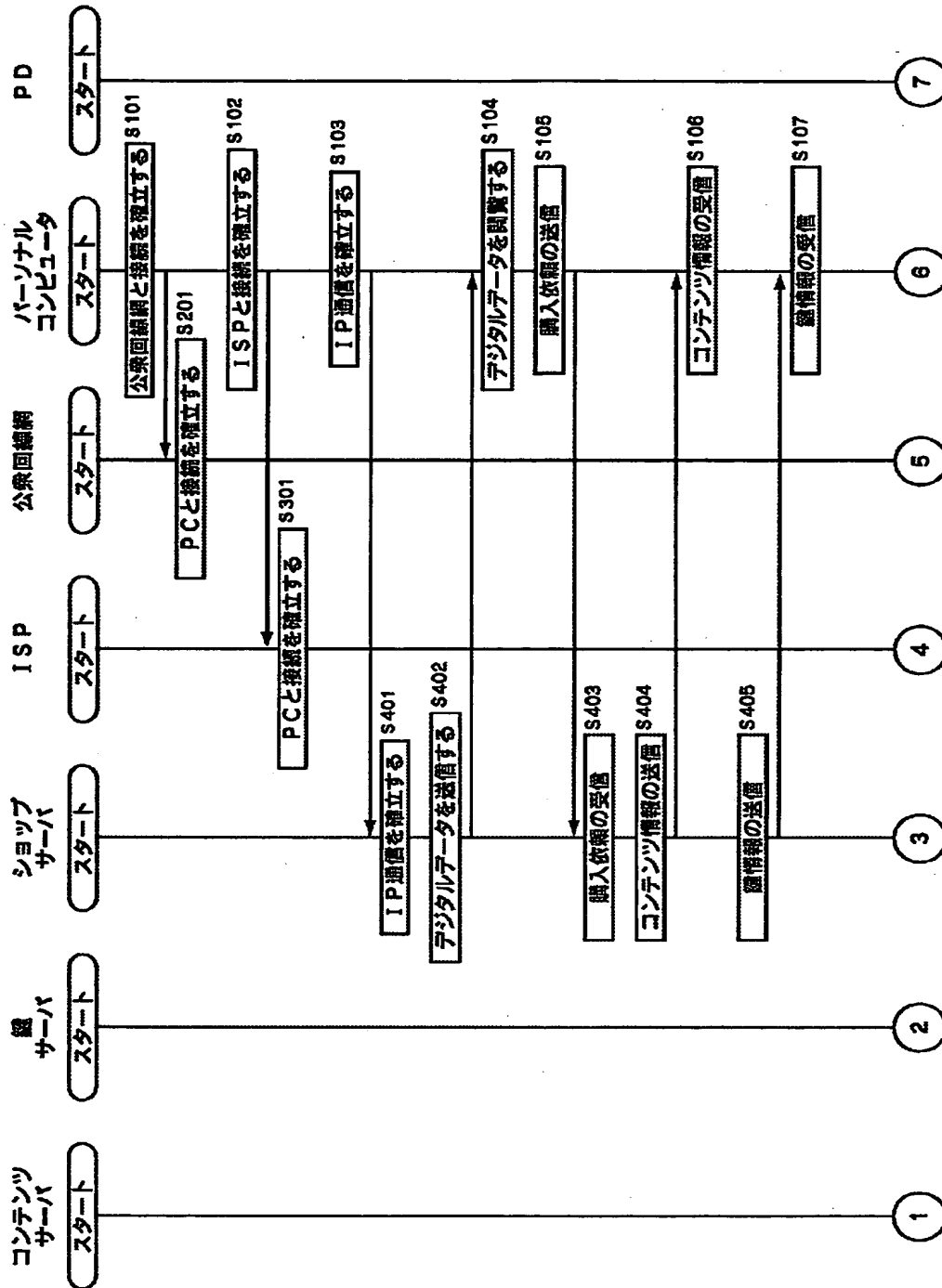


【図2】



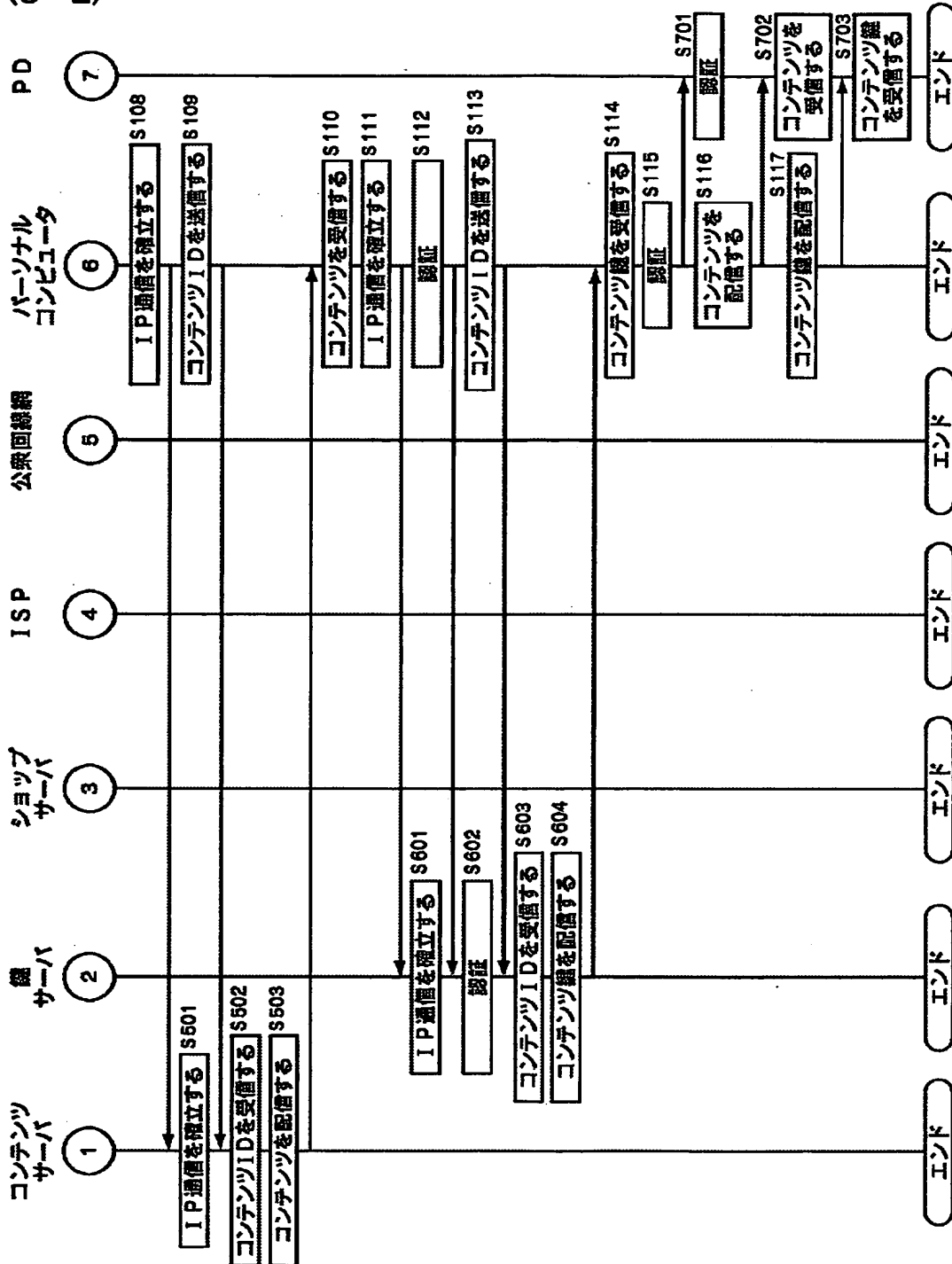
【図 3】

(3-1)

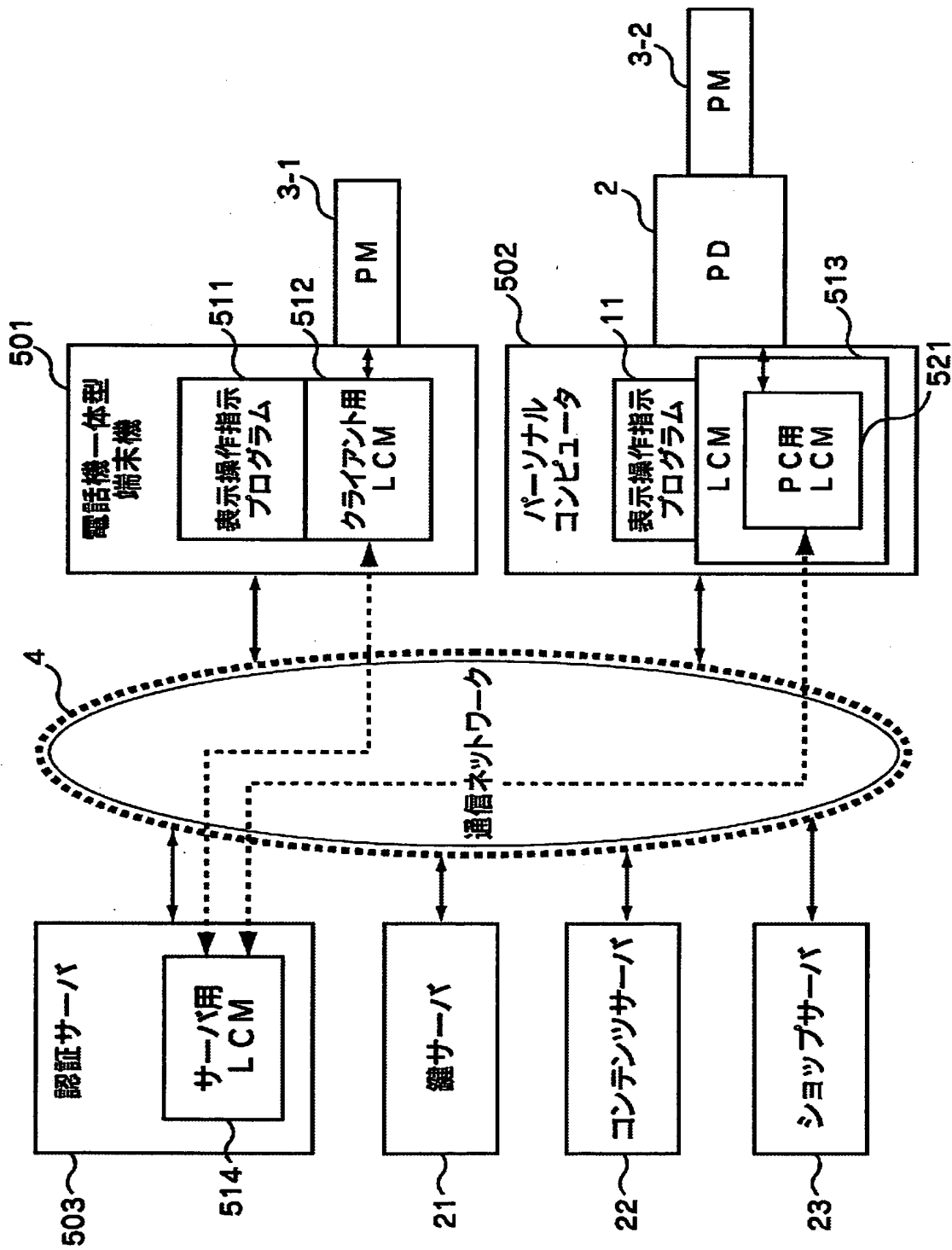


【图4】

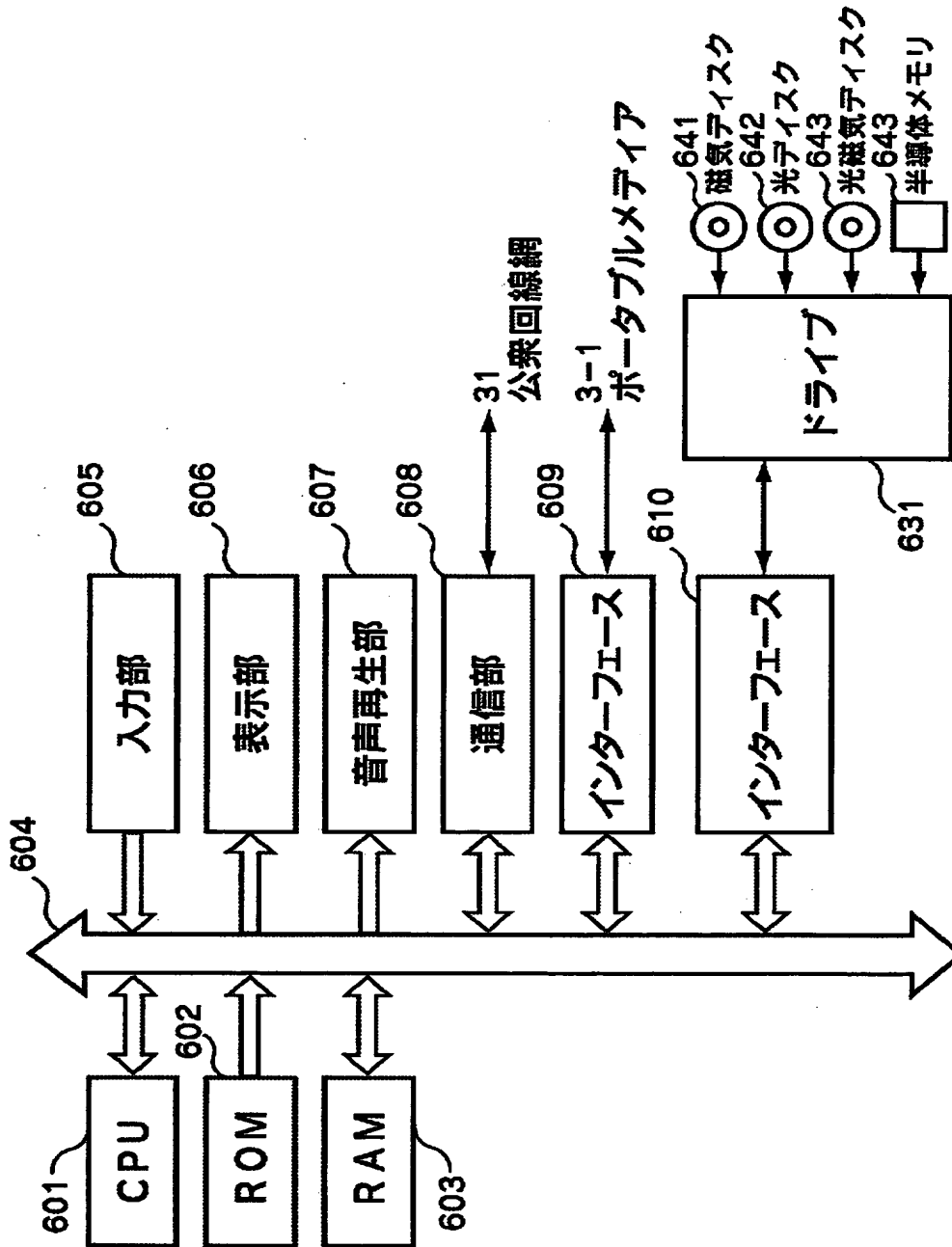
**(3-2)**



【図 5】

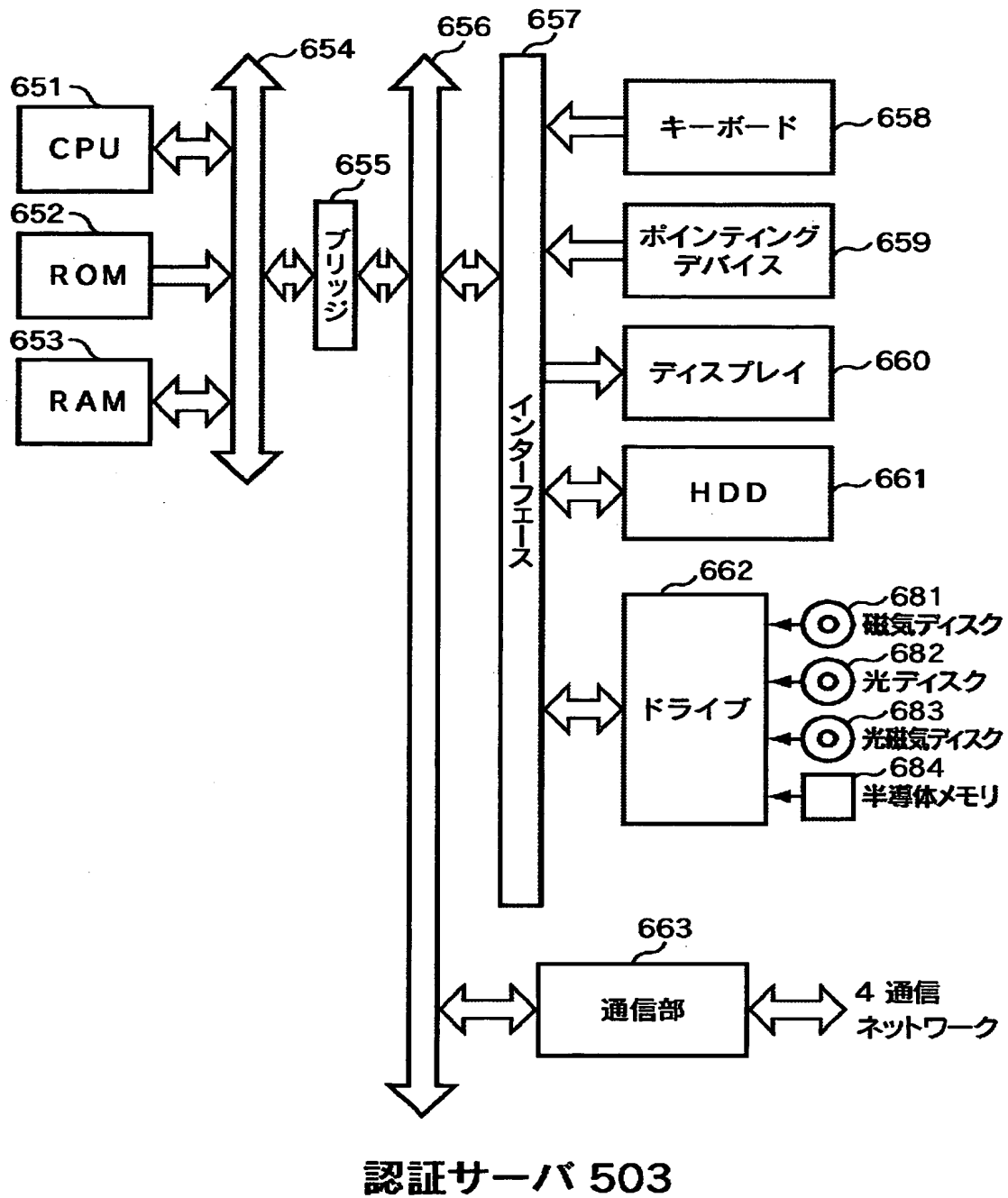


【図 6】

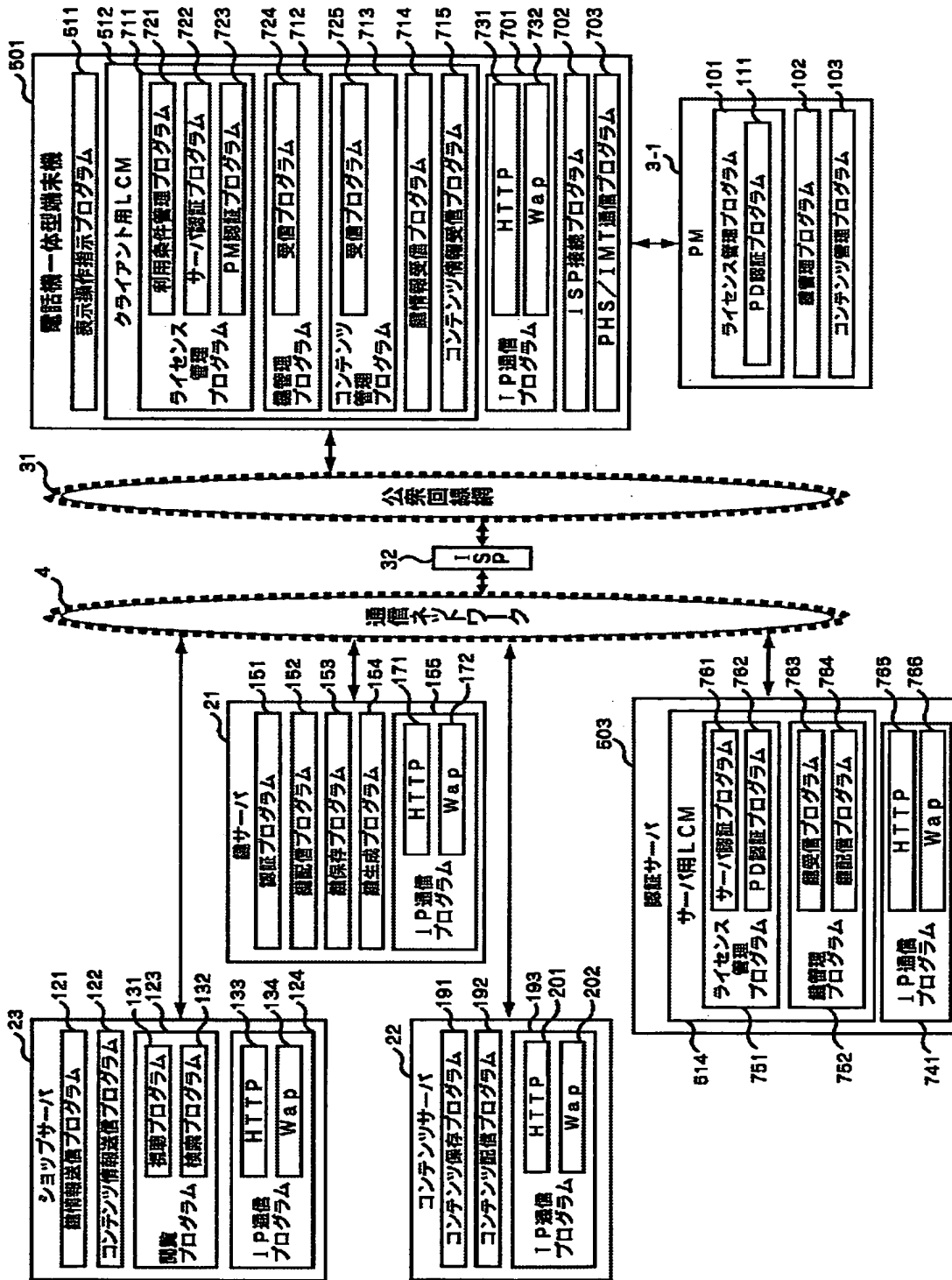


電話機一体型端末機 501

【図 7】

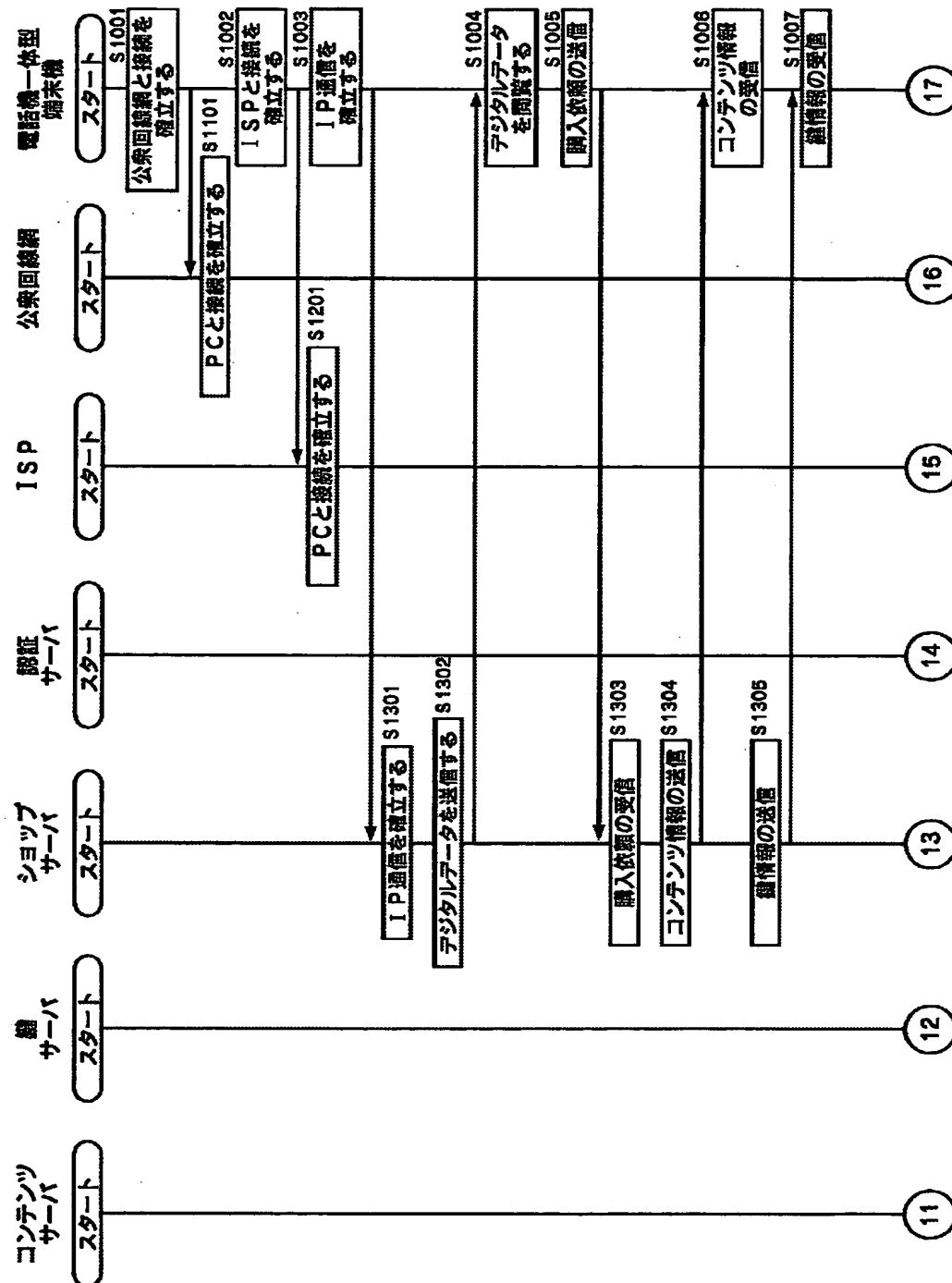


【図 8】



【図 9】

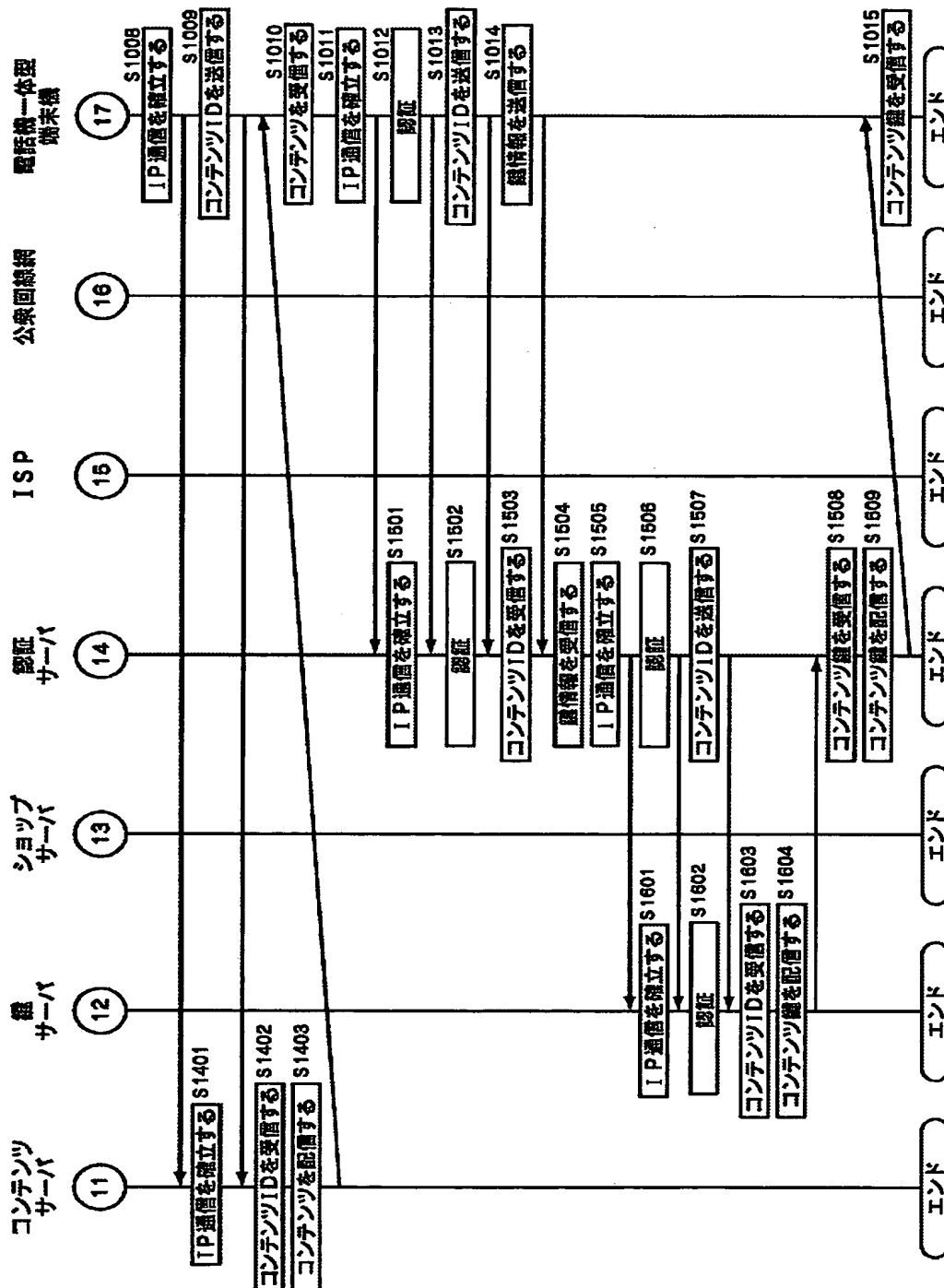
(9-1)





【図 10】

(9-2)



【書類名】 要約書

【要約】

【課題】 不正なコンテンツの利用を防止しつつ、迅速に、コンテンツをダウンロードする。

【解決手段】 PD認証プログラム762は、電話機一体型端末機501を認証する。サーバ認証プログラム761は、鍵サーバ21を認証する。サーバ用LCM514は、電話機一体型端末機501からの、鍵サーバ21を特定するデータおよび鍵の要求の受信を制御する。サーバ用LCM514は、鍵サーバ21を特定するデータに基づき、鍵サーバ21に鍵の要求を送信するとともに、鍵サーバ21から鍵を受信するように通信を制御する。鍵配信プログラム764は、電話機一体型端末機501への鍵の送信を制御する。

【選択図】 図8

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社